UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,043	12/01/2003	Ryhwei Yeh	5670-33	2981

20792 7590 09/30/2008
MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
YOUSEFI, SHAHROUZ	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
09/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,043	YEH ET AL.	
	Examiner	Art Unit	
	SHAHROUZ YOUSEFI	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/09/2007, 04/14/2005 and 09/13/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-5, 7-10, 12-14 and 16-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Toh et al. (US 2002/0019932) hereinafter Toh in view of Medvinsky (US 2002/0146132).

3. With respect to claim 1, Toh discloses a method of rekeying (provide...a different public key from a different private-public key pair, par. [0064]) in an authentication system (fig. 1) including an authenticated data processing system (access system 300, fig. 6) and an authenticating data processing system (switch system 310, fig. 6), comprising the following carried out by the authenticating data processing system: detecting failure (switch system 310 returns 650B an acknowledgement that the authentication failed, par. [0064] and fig. 6) of an authentication of the authenticated data processing system with a current public key associated with the authenticated data processing system (authenticating the first access system using the public key associated with the first access key, claim 1); and updating the current public key associated with the authenticated data processing system with an updated public key responsive to detecting failure of an authentication of the authenticated data processing system with the current public key (As a result of the failed authentication...provide the

switch system with a different public key from a different private-public key pair (redo steps 500 and 505, fig. 5), par. [0064). Toh doesn't disclose automatically updating the current public key. However, Medvinsky teaches such a feature (The client is able to automatically request a new ticket from a key distribution center in response to a successful authentication of the error message, see abstract and par. [0014]). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Toh by automatic key updating capability as taught in Medvinsky to enable client to automatically recover and be successfully authenticated by the authentication system.

4. With respect to claim 2, Medvinsky discloses the authentication system comprises a server-side authentication system (As an example, if a client wishes to access an application server, a third party authentication service can validate the client, par. [0003]), the authenticated data processing system comprises an authenticated server (the server initially pre-register with the third party authentication service, par. [0003]) and the authenticating data processing system comprises a client of the authenticated server (the client and the server initially pre-register, par. [0003]), and wherein detecting failure comprises detecting failure of an authentication of the authenticated server with a current public key associated with the authenticated server (error message … sent back to the client, par. [0041] and fig. 2); and wherein automatically updating comprises automatically updating the current public key associated with the authenticated server with an updated public key responsive to detecting failure of an authentication of the authenticated server with the current public

key (this error causes the client to request a new ticket…with the currently valid service, version V+1, par. [0043] and fig. 2).

5. With respect to claim 3, Toh discloses detecting failure of an authentication of the authenticated server comprises: receiving a signed certificate from the authenticated server; and failing to verify the signed certificate with the current public key (as a result of the failed authentication … provide the switch system with a different public key from a different private-public key pair (redo steps 500 and 505, fig. 5), par. [0064]).

6. With respect to claim 4, Medvinsky discloses automatically updating the current public key associated with the authenticated server comprises: establishing a connection to an authentication server (fig. 2, item 104); requesting the updated public key from the authentication server over the established connection (Service key update, item 205, fig. 2); receiving the updated public key over the established connection (return a new ticket, item 213, fig. 2); and replacing the current public key at the client with the received updated public key (fig. 2).

7. With respect to claim 5, Toh discloses establishing a connection to the authentication server comprises establishing a secure connection to the authentication server (a secure connection enabled application, abstract and par. [0012]).

8. With respect to claim 7, Toh discloses the authenticated server and the authentication server comprise a single server (securely transmitting data via a single node (310), par. [0013]).

9. With respect to claim 8, Medvinsky discloses requesting the updated public key from the authentication server comprises sending a request for an updated public key to

the authentication server, the request including an identification of the current public key (fig. 2).

10. With respect to claim 9, Toh discloses the identification of the current public key comprises a checksum of the current public key (data file 601 could be hashed, par. [0065] and par. [0033]).

11. With respect to claim 10, Toh discloses receiving the updated public key comprises: receiving the updated public key signed with a private key corresponding to the current public key; and verifying a signature of the received signed updated public key with the current public key (As a result of the failed authentication...provide the switch system with a different public key from a different private-public key pair (redo steps 500 and 505, fig. 5), par. [0064).

12. With respect to claim 12, Toh discloses the authenticated data processing system comprises a client and the authenticated data processing system comprises a server (the application proxies 1000 can be client based or server based, par. [0085]).

13. The subject-matter of independent claims 13, 27, 34, 36 and 38 corresponds to subject-matter of claim 1. Therefore, claims 13, 27, 34, 36 and 38 are rejected on the same rationale as to claim 1.

14. Claims 14, 16 and 17 correspond to claims 5, 8 and 9; therefore, claims 14, 16 and 17 are rejected on the same rationale as above.

15. With respect to claim 18, Medvinsky discloses validating the client as authorized to request an updated public key based on the identification of the current public key of

the client (authentication service can validate the client's identity to determine whether the client is authorized to access the application server, par. [0003]).

16. With respect to claim 19, Toh discloses selecting a private key from a repository of public/private key pairs based on the identification of the current public key (par. [0029]); and wherein providing the updated public key further comprises: signing the updated public key utilizing the selected private key (the sender has digitally signed the data, par. [0030]); and sending the signed updated public key to the client over the secure connection (a secure connection module 403, par. [0037]).

17. With respect to claim 20, Toh discloses storing the current public/private key pair of the server in a key repository (the key module 401 stores or otherwise accesses a private-public key pair of the user of an access system, par. [0040]).

18. With respect to claim 21, Toh discloses signing an authentication certificate of the server with the updated private key (The key module 401 can make the public key available to the switch system 310 by sending the public key or a digital certificate to the switch system 310 or publishing the key or the certificate to a generally accessible public key database or directory 415, par. [0042]).

19. With respect to claim 22, Medvinsky discloses automatically requesting updating of the current public key of the client associated with the server with an updated public key responsive to detecting failure of an authentication of the server with the current public key (system for seamlessly updating service key with automatic recovery, title).

20. Claims 23-25 correspond to claims 3, 9 and 10; therefore, claims 23-25 are rejected on the same rationale as above.

21. With respect to claim 28, Toh discloses a key repository operably associated with the authentication server, the key repository being configured to store previous public/private key pairs associated with the authenticated server (Key Module (411) and storage area (416), fig. 4).

22. With respect to claim 29, Toh discloses the authentication server is further configured to select a public/private key pair from the key repository corresponding to a current public key of the first client from which a request was received and sign the updated public key with a private key of the selected public/private key pair (par. [0063] and Fig. 4).

23. With respect to claim 30, Toh discloses the first client is further configured to receive the updated public key from the authentication server and to verify a signature of the received updated public key with the current public key of the first client (As a result of the failed authentication...provide the switch system with a different public key from a different private-public key pair (redo steps 500 and 505, fig. 5), par. [0064).

24. With respect to claim 31, Toh discloses a second client (a second access system 320, par. [0035]) configured to detect failure of the second client to authenticate an authenticated server and automatically request an updated public key associated with the authenticated server for which authentication failure was detected; and wherein the authentication server is further configured to receive requests for updated public keys from the second client and send updated public keys to the second client (As a result of the failed authentication...provide the switch system with a different public key from a different private-public key pair (redo steps 500 and 505, fig. 5), par. [0064).

25. With respect to claim 32, Toh discloses the authentication server is further configured to select a public/private key pair from the key repository corresponding to a current public key of the first client from which the request was received and sign the updated public key with a private key of the selected public/private key pair and to select a public/private key pair from the key repository corresponding to a current public key of the second client from which the request was received and sign the updated public key with a private key of the selected public/private key pair (Using access system 300 as an example, the key module 401 stores or otherwise accesses a private-public key pair of the user of an access system. The key module 401 can also be configured to store or access multiple key pairs of a single or of multiple users, par. [0040].

26. With respect to claim 33, Toh discloses the selected public/private key pair from the key repository corresponding to a current public key of the second client and the selected public/private key pair from the key repository corresponding to a current public key of the first client are different public/private key pairs (Using access system 300 as an example, the key module 401 stores or otherwise accesses a private-public key pair of the user of an access system, par. [0040]).

27. Claims 35 and 37 correspond to claim 2; therefore, claims 35 and 37 are rejected on the same rationale as to claim 2.

28. With respect to claim 39, Toh discloses the authenticated communication comprises a signed certificate, the authenticating data processing system comprises a client and the source of the authenticated communication comprises a server (The key

module 401 can make the public key available to the switch system 310 by sending the public key or a digital certificate to the switch system 310 or publishing the key or the certificate to a generally accessible public key database or directory 415, par. [0042]).

29. With respect to claim 40, Toh discloses the authenticated communication comprises a signed certificate, the authenticating data processing system comprises a server and the source of the authenticated communication comprises a client (The key module 401 can make the public key available to the switch system 310 by sending the public key or a digital certificate to the switch system 310 or publishing the key or the certificate to a generally accessible public key database or directory 415, par. [0042]).

30. With respect to claim 41, Toh discloses the authenticated communication comprises an e-mail message, wherein the authenticating data processing system comprises a mail recipient and the source of the authenticated communication comprises a source of the e-mail message (An example of an application proxy includes an email application proxy that redirects all outgoing SMTP (Simple Mail Transfer Protocol) traffic to the switch system 310 for delivery, and then translates all incoming traffic from the switch system 310 prior to it being routed to internal email).

31. With respect to claim 42, Toh discloses the source of the e-mail message comprises an author of the e-mail (user email address, par. [0046]).

32. With respect o claim 43, Toh discloses the source of the e-mail message comprises an e-mail server (par. [0083]).

33. Claims 6, 15, 11 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Toh et al. (US 2002/0019932) hereinafter Toh in view of Medvinsky (US 2002/0146132) and further in view of Smith et al. (US 6, 532,543) hereinafter Smith.

34. With respect to claim 6 and 15, Toh and Medvinsky don't disclose the secure connection comprises a Secure Sockets Layer encryption only connection. However, Smith teaches secure methods comprising key-escrow encapsulated within an application program interface ("API") such as a Secure Socket Layer, col. 10, lines 50-53. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Toh and Medvinsky with SSL of Smith to provide a secure channel between client and server.

35. With respect to claims 11 and 26, Smith discloses the authenticated server comprises a system monitoring server (a corresponding message is transmitted to monitor node 674, as shown by step 1022, col. 22, lines 12-13) and the client comprises a resource monitoring agent (the installation server has verified that the agent module is installed on the proper target site, col. 22, lines 16-17). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Toh and Medvinsky with monitoring capability of Smith to detect and prevent unauthorized access to the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHAHROUZ YOUSEFI whose telephone number is

(571) 270-3558. The examiner can normally be reached on Monday-Thursday 9:00-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. Y./
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132